APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/587,308	02/26/2007	Jun Furukawa	20111	4530

23389   7590   11/10/2010
SCULLY SCOTT MURPHY & PRESSER, PC
400 GARDEN CITY PLAZA
SUITE 300
GARDEN CITY, NY 11530

EXAMINER
POWERS, WILLIAM S

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
11/10/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 July 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   The Examiner has stated the below column and line numbers as examples. All columns and line numbers in the reference and the figures are relevant material and Applicant should take the entire reference into consideration upon the reply to this Office Action.

2.   Claims 1-10 are pending.

Information Disclosure Statement

3.   The Information Disclosure Statement submitted 8/31/2006 has been considered by the Examiner.

Claim Objections

4.   Claims 1-10 are objected to because of the following informalities, the claims appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors. The Examiner has tried to find all the errors and detailed them below with the interpretation of the language, if necessary, used in the rejecting the limitations. The errors listed are not exhaustive and the Applicant is required to correct any errors that may have been overlooked.

a.   As to claim 1, the limitation in lines 5-6 is interpreted as,

"characterized in that the input process inputs to a circuit of each of the

plurality of computers an input bit." The term "calculation" in line 7 needs

an article. The limitation, "the calculation result" lines 7-8, lacks

antecedent basis. Examiner assumes "the value" was intended. The

second instance of "calculation" is interpreted as "the next calculation".

The term "calculation" (twice in line 11 and twice in line 13) is assumed to

have the article "the" before each instance of the term "calculation".

b.   As to claim 2, the limitation "and information on the plurality of

computers" in line 9 is redundant as the information is already inputted to

a circuit on each of the plurality of computers. The limitation "the function"

in line 11 lacks antecedent basis. It is read as "the given function". The

limitation, "this turn" lacks antecedent basis. The limitation, "the set of

cipher texts" in line 22 is read as "the set of ElGamal cipher texts". The

limitation "the next order" in lines 25-26 lacks antecedent basis.

c.   As to claim 3, the limitation "the given function" in line 14 lacks

antecedent basis. It is read as "the function". The limitation "in this turn" in

line 16, lacks antecedent basis. The limitation, "the set of cipher texts" in

line 18 is read as "the set of ElGamal cipher texts". The limitation "the next

order" in lines 22 lacks antecedent basis.

d.   As to claim 4, the phrase, "the gate" in line 4 is read as "the gates".

Lines 3-4 are read as, "of the gates is a set of ElGamal cipher texts of a

secret key, corresponding to each of the gates, generated by each of the

computers. The limitation, "two signals input" in line 6 is read as "two signal inputs". The limitation, "this gate", lacks antecedent basis.

e.   As to claim 5, the limitation "the public key" in line 23 is read as "the input gate public key". The limitation "this computer" in line 33 lacks antecedent basis. The limitation "enciphering the gate secret key" in line 33 is read as "enciphering the gate secret key cipher text". The limitation "the circuit input" in line 43 lacks antecedent basis. There is a period at the end of line 43, it has been ignored.

f.   As to claim 6, the term "calculation" in line 2 is read as "a calculation". The limitation "the calculation result" in line 3 lacks antecedent basis. The limitation "calculation" in line 5 is read as "the next calculation". Each instance of the limitation "calculation" in lines 6-8 is read as "the calculation". The limitation, "the main calculation" in lines 21, 32, 36 and 39-40 lacks antecedent basis. The limitation "from other computer" in line 23 is read as "from a previous computer". The limitation "from the other computer" in line 26 is read as "from the previous computer".

g.   As to claim 7, the limitation "a data main body" in line 1 is read as "the data main body". The limitation, "the main calculation" in line 3 lacks antecedent basis.

h.   As to claim 8, the limitation "the calculation means" in line 4 is read as "the calculation means for the first cycle". The limitation "the calculation means of the zero-th cycle" in line 7 lacks antecedent basis. The limitation

"the cipher texts" in lines 12-13, 18 and 26 lacks antecedent basis. The

limitation "the calculation result" in lines 26 and 28 lacks antecedent basis.

i.   As to claim 9, delete "of" in line 2. The limitation "the second cycles"

in lines 3 and 10 is read as "the second cycle". The limitation, "the main

calculation" in line 6 lacks antecedent basis. The limitation, "the calculation

means of the second cycle cipher text conversion means" in line 10 lacks

antecedent basis.

j.   As to claim 10, the limitation, "the main calculation means" is read

as "the main calculation calculating means".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and
> process of making and using it, in such full, clear, concise, and exact terms as to enable any
> person skilled in the art to which it pertains, or with which it is most nearly connected, to make
> and use the same and shall set forth the best mode contemplated by the inventor of carrying
> out his invention.

6.   Claims 1-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to

comply with the enablement requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to enable one

skilled in the art to which it pertains, or with which it is most nearly connected, to

make and/or use the invention. The limitations of claims 1-10, as presently

written, do not include a stopping condition. Without a stopping condition, the

method and system of the instant application would run in perpetuity as output

from one computer becomes input to the next computer.

7.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

8.   Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention.

As to claim 6, the limitation "the calculation of the zero-th cycle is

performed before the first computer performs the calculation of the first cycle" in

lines 13-14 of the claim is indefinite as it is not clear when and with what

computers the calculation of the zero-th cycle occurs. It is not clear if there is

another computer not used in the first cycle that makes the calculation of the

zero-th cycle or if there is preprocessing of the input data that is input to the first

computer. The limitation, "the main calculation calculates the random number

generated by the random number generating means" implies that the main

calculation means generates the same random number as the random number

generating means. The Examiner assumes that the main calculation calculates

with the random number generated by the random number generating means.

9.   Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention. The claim recites the following means

plus function limitation: "first computer special calculating means". The Examiner

could find no algorithm relating to the first computer special calculating means of

the claim limitations.

This limitation invokes 35 USC §112, ¶6 because it meets the 3-prong

analysis set forth in MPEP 2181 as it recites the phrase "means for" and the

phrase is modified by functional language and it is not modified by sufficient

structure, material or acts for performing the recited function. Also see *Altiris Inc.*

v. Semantec Corp., 318 F.3d 1363, 1375 (Fed. Cir. 2003). 35 USC §112, ¶6,

requires such claim to be construed to cover the corresponding structure,

material or acts described in the specification and equivalents thereof. "If one

employs means plus function language in a claim, one must set forth in the

specification an adequate disclosure showing what is meant by that language. If

an applicant fails to set forth an adequate disclosure, the applicant has in effect

failed to particularly point out and distinctly claim the invention as required by the

second paragraph of section 112." *In re Donaldson Co.*, 16 F.3d 1189, 1195, 29

USPQ, 1845, 1850 (Fed. Cir. 1994) (in banc.). For a computer-implemented

means-plus-function claim limitation that invokes 35 USC §112, ¶6, the

corresponding structure is required to be more than simply a general purpose

computer. *Aristocrat Technologies, Inc. v. International Game Technology*, 521

F.3d 1328, 1333, 86 USPQ2d 1235, 1239-40 (Fed. Cir. 2008). The

corresponding structure for a computer-implemented function must include the

algorithm as well as the general purpose computer. WMS Gaming, Inc. v.

International Game Technology, 184 F.3d 1339, 51 USPQ2d 1385 (Fed. Cir.

1999). The written description must at least disclose the algorithm that

transforms the general purpose microprocessor into a special purpose computer

programmed to perform the claimed function. *Aristocrat*, 521 F.3d at 1338, 86

USPQ2d at 1242.

It is noted that support for the other means plus function limitations in

claims 3, 6 and 8 was found throughout the specification and figures.

Claim Rejections - 35 USC § 102

10.   The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11.   Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by "The

Round Complexity of Secure Protocols" by Beaver et al. (hereinafter Beaver).

As to claim 1, Beaver teaches:

a.   An input process (input tape for each processor) (Beaver, p. 505,

col. 2, 6th paragraph).

b.   An output process (output tape for each processor) (Beaver, p. 505,

col. 2, 6th paragraph).

c.   Characterized in that the input process inputs to a circuit an input

bit to the circuit to the plurality of computers (input tape for each

processor) (Beaver, p. 505, col. 2, 6th paragraph).

d.   One of the computers firstly performs a calculation and transmits

the calculation result to another computer and the another computer which

has received the calculation result performs the next calculation such that

calculation is performed by one computer after another, and when all the

computers have performed calculation once, the last computer which has

performed the calculation transmits the calculation result to the first

computer which has performed calculation, and after this, calculation is

performed by one computer after another and the calculation result is

transmitted to the next computer such that the calculation of each cycle is

repeated (each round a processor that is part of a network of processors,

performs calculations on the data output by the previous processor)

(Beaver, p. 505, Model of computation section).

Claim Rejections - 35 USC § 103

12.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

13.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1,

148 USPQ 459 (1966), that are applied for establishing a background for

determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness or nonobviousness.

14.   This application currently names joint inventors. In considering

patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that

the subject matter of the various claims was commonly owned at the time any

inventions covered therein were made absent any evidence to the contrary.

Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor

and invention dates of each claim that was not commonly owned at the time a

later invention was made in order for the examiner to consider the applicability of

35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35

U.S.C. 103(a).

15.   Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Applicant admitted prior art "The Round Complexity of Secure Protocols" by

Beaver et al. (hereinafter Beaver) in view of US Patent Application Publication

No. 2002/018172 to Furukawa.

As to claim 2, Beaver teaches:

a.   An input process (input tape for each processor) (Beaver, p. 505,

col. 2, 6th paragraph).

Beaver does not expressly mention an ElGamal cipher text preparation process.

However, in an analogous art, Furukawa teaches:

b.   An ElGamal cipher text preparation process (text is processed

before inputting, in this case encrypted using the ElGamal protocol)

(Furukawa, [0047-0048 and 0066-0078]).

Therefore, one of ordinary skill in the art at the time the invention was

made would have been motivated to implement the networked processor

computation protocol of Beaver with the ElGamal algorithm of Furukawa in order

increase the efficiency of encryption/decryption systems as suggested by

Furukawa (Furukawa, [0019]).

Beaver as modified further teaches:

c.   A sequential substitution reencryption process (shuffling the

encrypted texts and reencrypting them) (Furukawa, [0005]).

d.   A result output process (output tape for each processor) (Beaver, p.

505, col. 2, 6th paragraph).

e.   Characterized in that the input process comprises an information

input step of inputting to the plurality of computers information on a

circuitry including a plurality of gates and information on the plurality of

computers, and a dispersion input step of inputting to each of the

computers each one of plural pieces of partial data which are obtained by

dispersing input data of the function into plural pieces by the number of the computers (first stage of the process is a sharing stage wherein the input is divided and distributed according to the number of "players" involved) (Beaver, p. 503, 3rd full paragraph).

f.   The ElGamal cipher text preparation process comprises an ElGamal cipher text preparation step of generating a set of ElGamal cipher texts in which at least one of the computers corresponds to the gate of the circuit that realizes the given function (a common circuit is used to process the inputs to the various players in the protocol) (Beaver, p. 504-505, A bird's-eye view of our solution section).

g.   The sequential substitution reencryption process comprises a step of allowing each of the computers perform a substitution reencryption process one after another, and the substitution reencryption process comprises a cipher text obtaining step of allowing the computer in this turn to receive the set of ElGamal cipher texts from the computer in the previous turn, a cipher text substitution and reencryption step of changing an order of the set of cipher texts received in the cipher text obtaining step for substitution and subjecting those cipher texts to reencryption (certified shuffling process) (Furukawa, [0047-0050]) and a step of disclosing the data generated in the cipher text substitution and reencryption step to at least the computer in the next order (the output of one processor is the input for the next processor) (Beaver, p. 505, Model of computation section).

h.   The result output process comprises a partial decryption step of

deciphering or partially deciphering a part of the cipher texts generated in

the cipher text substitution and reencryption step, a decryption step of

deciphering a cipher text that enciphers data corresponding to the input to

the circuit in the cipher texts generated in the cipher text substitution and

reencryption step, and an evaluation step of evaluating an output of the

circuitry by using the data deciphered in the decryption step and the data

partially deciphered in the partial decryption step (decrypted texts and

shuffle or partial decrypted are compared for validation purposes)

(Furukawa, [0052]).

As to claim 3, Beaver teaches:

a.   A plurality of computers (network of processors) (Beaver, p. 505,

Model of computation section).

b.   Communication means for performing communication with the

plurality of computers (communication channels exist between the

processors) (Beaver, p. 505, Model of computation section).

c.   Input process means (input tape for each processor) (Beaver, p.

505, col. 2, 6th paragraph).

Beaver does not expressly mention an ElGamal cipher text preparation process.

However, in an analogous art, Furukawa teaches:

d.   ElGamal cipher text preparation means (text is processed before

inputting, in this case encrypted using the ElGamal protocol) (Furukawa,

[0047-0048 and 0066-0078]).

Therefore, one of ordinary skill in the art at the time the invention was

made would have been motivated to implement the networked processor

computation protocol of Beaver with the ElGamal algorithm of Furukawa in order

to increase the efficiency of encryption/decryption systems as suggested by

Furukawa (Furukawa, [0019]).

Beaver as modified further teaches:

e.   Sequential substitution reencryption means (shuffling the encrypted

texts and reencrypting them) (Furukawa, [0005]).

f.   Result output means (output tape for each processor) (Beaver, p.

505, col. 2, 6th paragraph).

g.   Characterized in that the input means inputs information on a circuit

whose output is desired to be obtained, information on the plurality of

computers, and information on which part of an input to the circuit each of

the computers has (first stage of the process is a sharing stage wherein

the input is divided and distributed according to the number of "players"

are involved) (Beaver, p. 503, 3rd full paragraph).

h.   The ElGamal cipher text preparation means prepares ElGamal

cipher texts for generating a set of ElGamal cipher texts corresponding to

gates of the circuit that realizes the given function (a common circuit is

used to process the inputs to the various players in the protocol) (Beaver,

p. 504-505, A bird's-eye view of our solution section).

i.   The sequential substitution reencryption means comprises cipher

text obtaining means for allowing the computer in this turn to receive the

set of ElGamal cipher texts from the computer in the previous turn, cipher

text substitution and reencryption means for changing an order of the set

of cipher texts received by the cipher text obtaining means for substitution

and subjecting those cipher texts to reencryption (certified shuffling

process) (Furukawa, [0047-0050]), and means for disclosing the data

generated by the cipher text substitution and reencryption means to at

least the computer in the next order (the output of one processor is the

input for the next processor) (Beaver, p. 505, Model of computation

section).

j.   The result output means comprises partial decryption means for

deciphering or partially deciphering a part of the cipher texts generated by

the cipher text substitution and reencryption means, decryption means for

deciphering encryption related to itself of a cipher text that enciphers data

corresponding to the input to the circuit in the cipher texts generated by

the cipher text substitution and reencryption means, and evaluation means

for evaluating an output of the circuit while using the data deciphered by

the decryption means by the plurality of computers and data partially

deciphered by the partial decryption means by the plurality of computers

(decrypted texts and shuffle or partial decrypted are compared for

validation purposes) (Furukawa, [0052]).

As to claim 4, Beaver does not expressly mention the generation of

public/private key pairs. However, in an analogous art, Furukawa teaches:

a.   Characterized in that the set of ElGamal cipher texts corresponding

to each of the gates is a set of ElGamal cipher texts of a secret key

generated corresponding to each of the gates by each of the computers

(domain parameters or secret keys are generated from two prime

numbers p and q) (Furukawa, [0067-0069]).

Therefore, one of ordinary skill in the art at the time the invention was

made would have been motivated to implement the networked processor

computation protocol of Beaver with the ElGamal key creation of Furukawa in

order increase the efficiency of encryption/decryption systems as suggested by

Furukawa (Furukawa, [0019]).

b.   A public key used for generating the ElGamal cipher texts is a sum

of public keys corresponding to gates for generating two signals input to

this gate (shuffling unit receives multiple public keys used for encryption)

(Furukawa, [0055]).

16.   Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Applicant admitted prior art "The Round Complexity of Secure Protocols" by

Beaver et al. (hereinafter Beaver) in view of US Patent Application Publication

No. 2002/018172 to Furukawa as applied to claim 2 above, and further in view of

US Patent No. 6,195,433 to Vanstone et al. (hereinafter Vanstone).

As to claim 5, Beaver as modified teaches:

a.   Characterized in that the input process further comprises a step of

inputting an area variable of an ElGamal encryption method to each of the

computers (random input string is selected for each player) (Beaver, p.

508, Pseudorandom generators section).

Beaver as modified teaches computing gate labels for each gate (Beaver, p.509),

but does not expressly mention the generation of public/private keys. However, in

an analogous art, Vanstone teaches:

b.   The ElGamal cipher text preparation process further comprises a

gate secret key generating step of generating a secret key of the ElGamal

cipher texts corresponding to each of the gates of the circuit by each of

the computers (generating a private key for an ElGamal algorithm)

(Vanstone, 3:13-36).

Therefore, one of ordinary skill in the art at the time the invention was

made would have been motivated to implement the networked processor

computation protocol of Beaver as modified with the key generation of Vanstone

in order to ensure randomness and validate key generation as suggested by

Vanstone (Vanstone, 1:1-10).

Beaver as modified further teaches:

c.   Each of the computers performs:

i.   A gate public key generating step of generating a gate public

key corresponding to the secret key generated in the gate secret

key generating step (public key counterpart is generated)

(Vanstone, 4:45-53).

ii.   A gate public key validity proof generating step of generating

a gate public key validity proof for the public key generated in the

gate public key generating step (key test processing) (Vanstone,

3:51-65).

iii.   An input gate secret key generating step of generating a

secret key of the ElGamal cipher texts corresponding to a gate

where an input is directly made to the circuit of the gates of the

circuit (generating a private key for an ElGamal algorithm)

(Vanstone, 3:13-36).

iv.   An input gate public key generating step of generating an

input gate public key corresponding to the secret key generated in

the input gate secret key generating step (public key counterpart is

generated) (Vanstone, 4:45-53).

v.   An input gate public key validity proof generating step of

generating a validity proof for the public key generated in the input

gate public key generating step (key test processing) (Vanstone,

3:51-65).

vi.   An input gate public key validity proof disclosing step of

disclosing the input public key validity proof generated in the input

gate public key validity proof generating step (keys are only

accepted if they fall within a predetermined acceptable range)

(Vanstone, 4:30-43).

vii.   A gate public key obtaining step of obtaining gate public

keys generated by other respective computers (shuffling unit

receives multiple public keys used for encryption) (Furukawa,

[0055]).

viii.   A gate public key integration step integrating the gate public

keys obtained in the gate public key obtaining step (shuffling unit

receives multiple public keys used for encryption) (Furukawa,

[0055]).

ix.   A gate public key encryption step of enciphering the gate

secret key cipher text generated by this computer with the gate

public key integrated in the gate public key integration step, a gate

secret key cipher text disclosing step of disclosing a gate secret key

cipher text generated in the gate public key encryption step, and a

gate secret key cipher text validity proof generating step of

generating a validity proof for the gate secret key cipher text (secret

key is subjected to tests and the plaintext of the private key is

recovered) (Vanstone, 4:45-5:5).

x.   An input cipher text generating step of generating a cipher

text corresponding to a part of the input of the circuit input to each

of the computer, an input cipher text validity proof generating step

of generating a validity proof for the cipher text corresponding to the

part of the input of the circuit generated in the input cipher text

generating step, an input cipher text validity proof disclosing step of

disclosing the proof generated in the input cipher text validity proof

generating step, and an output cipher text generating step of

generating and disclosing a cipher text corresponding to an output

of the gate (input of the circuit is processed and tested for validity)

(Beaver, pp. 509-510, Phase II section).

    d.   The sequential substitution reencryption process comprises:

        i.   A gate secret key cipher text substitution and reencryption

step of changing an order of a set of the input cipher texts with one

substitution randomly selected on the basis of a predetermined

permitted substitution method for reencryption (decrypted texts and

shuffle or partial decrypted are compared for validation purposes)

(Furukawa, [0052]).

        ii.   An input cipher text substitution and reencryption step of

changing an order of a set of the input cipher texts with one

substitution randomly selected on the basis of a predetermined

permitted substitution method for reencryption (decrypted texts and

shuffle or partial decrypted are compared for validation purposes)

(Furukawa, [0052]).

        iii.   An output cipher text substitution and reencryption step of

changing an order of a set of the output cipher texts with one

substitution randomly selected on the basis of a predetermined

permitted substitution method for reencryption (decrypted texts and

shuffle or partial decrypted are compared for validation purposes)

(Furukawa, [0052]).

iv.   A gate secret key cipher text, input cipher text, and output

cipher text substitution and reencryption validity proof generating

and disclosing step of generating and disclosing validity proofs for

the substitution and reencryption performed in the gate secret key

cipher text substitution and reencryption step, the input cipher text

substitution and reencryption step and the output cipher text

substitution and reencryption step (decrypted texts and shuffle or

partial decrypted are compared for validation purposes) (Furukawa,

[0052]).

e.   The partial decryption step of the result output process comprises:

a gate secret key partial decryption step of partially deciphering the gate

secret key cipher texts by mutually performing communication and

calculation by the computers, an input cipher text partial decryption step of

partially deciphering the input cipher texts by mutually performing

communication and calculation by the computers, an output cipher text

partial decryption step of partially deciphering the output cipher texts by

mutually performing communication and calculation by the computer and a

gate secret key, input cipher text and output text partial decryption step

validity proof generating and disclosing step of generating and disclosing

the validity proofs for the partial decryption performed in the gate secret

key partial decryption step, the input cipher text partial decryption step and

the output cipher text partial decryption step (decrypted texts and shuffle

or partial decrypted are compared for validation purposes) (Furukawa,

[0052]).

    f.   The calculation method further comprises a step of verifying various

validity proofs disclosed by other computers (the players can check each

others computations) (Beaver, p. 507, Verifiable Secret Sharing section).

17.   Claims 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Applicant admitted prior art "The Round Complexity of Secure Protocols" by

Beaver et al. (hereinafter Beaver) in view of US Patent Application Publication

No. 2002/018172 to Furukawa and further in view of US Patent No. 6,195,433 to

Vanstone et al. (hereinafter Vanstone).

    As to claim 6, Beaver teaches:

    a.   A plurality of computers (network of processors) (Beaver, p. 505,

Model of computation section).

    b.   Input means (input tape for each processor) (Beaver, p. 505, col. 2,

6th paragraph).

    c.   Output means (output tape for each processor) (Beaver, p. 505,

col. 2, 6th paragraph).

d.   In which one of the computers firstly performs calculations and transmits the calculation result to another computer and the another computer which has received the calculation result performs the next calculations such that calculation is performed by one computer after another, and when all the computes have performed calculation once, the last computer which has performed calculation transmits the calculation result to the first computer which has performed calculation, and after this, calculation is performed by one computer after another and the calculation result is transmitted to the next computer such that the calculation of each cycle is repeated (each round a processor that is part of a network of processors, performs calculations on the data output by the previous processor) (Beaver, p. 505, Model of computation section).

e.   Characterized in that the input means inputs information on a circuit and a part of input bits to the circuit to the computer (first stage of the process is a sharing stage wherein the input is divided and distributed according to the number of "players" involved) (Beaver, p. 503, 3rd full paragraph).

f.   The calculation of the zero-th cycle is performed before the first computer performs the calculation of the first cycle (data is prepared before the first cycle) (Beaver, p. 509, Phase I).

g.   The plurality of computers comprise data obtaining means for obtaining transmitted data used in the calculation of each cycle (output of

one processor is input to the next processor) (Beaver, p. 505, col. 2, 6th

paragraph).

Beaver teaches verifiable secret sharing, but does not expressly mention a

validity proof. However, in an analogous art, Furukawa teaches validity proof

verifying means (validation certificates of the cyclic calculations) (Furukawa,

[0046-0052]).

Therefore, one of ordinary skill in the art at the time the invention was

made would have been motivated to implement to implement the networked

processor computation protocol of Beaver with the certificate of validation of the

cyclic calculations of Furukawa in order to increase the efficiency and security of

encryption/decryption systems as suggested by Furukawa (Furukawa, [0019]).

Beaver as modified does not expressly mention verifying signatures.

However, in an analogous art, Vanstone teaches signature text verifying means

(digital signatures are used for security purposes) (Vanstone, 1:30-58 and 5:31-

54).

Therefore, one of ordinary skill in the art at the time the invention was

made would have been motivated to implement to implement the networked

processor computation protocol of Beaver as modified with the signature

verification of Vanstone in order to increase the security of the system as

suggested by Vanstone (Vanstone, 5:31-40).

Beaver as modified further teaches:

First computer special calculating means preformed by the first computer

(private key seed is generated) (Vanstone, 3:37-45), random number generating

means for performing random number generation (RNG) (Vanstone, 3:37-45), a

main calculation calculating means for performing a main calculation (calculating

private key) (Vanstone, 3:37-45), validity proof generating means for proving a

validity for a calculation performed in the main calculation(validation certificates

of the cyclic calculations) (Furukawa, [0046-0052]), signature means (digital

signatures are used for security purposes) (Vanstone, 1:30-58 and 5:31-54) and

data transmission means (network of processors) (Beaver, p. 505, Model of

computation section).

> h.   The transmitted data comprises data transmitted from other
>
> computer, data main body, a validity proof for the data main body and a
>
> signature text (message, validation certificate and signature are
>
> transmitted from one computer to another) (Beaver, p. 505, Model of
>
> computation section; Furukawa, [0047-0050] and Vanstone, 5:31-54).
>
> i.   The signature text comprises data including a signature text
>
> corresponding to a combination of the data transmitted from the other
>
> computer, the data main body and the validity proof for the data main body
>
> (signature is based on content of the message) (Vanstone, 1:40-50).
>
> j.   The validity proof verifying means verifies a validity proof in the
>
> transmitted data (validation certificates verify the messages that are
>
> shuffled) (Furukawa, [0046-0050]).
>
> k.   The signature text verifying means verifies the signature text in the
>
> transmitted data (signature is based on content of the message)
>
> (Vanstone, 1:40-50).

l.   The main calculation calculates the random number generated by
the random number generating means (RNG) (Vanstone, 3:37-45).

m.   The signature means generates a signature text for a combination
of the transmitted data, the data main body that is the calculation result
calculated in the main calculation, and the validity proof generated by the
validity proof generating means (signature is based on content of the
message) (Vanstone, 1:40-50).

n.   The data transmission means transmits a combination of the
transmitted data, the data main body that is the calculation result
calculated in the main calculation, the validity proof generated by the
validity proof generation means and the signature text generated by the
signature means (message, validation certificate and signature are
transmitted from one computer to another) (Beaver, p. 505, Model of
computation section; Furukawa, [0047-0050] and Vanstone, 5:31-54).

As to claim 7, Beaver as modified teaches wherein a data main body of
the transmitted data and the data main body that is the calculation result
calculated in the main calculation comprise a combination of multiple sequence
alignment ElGamal cipher texts on a true value group ring and extended multiple
sequence alignment ElGamal cipher texts on the true value group ring in the
calculation of the first cycle (elliptic curve ElGamal scheme is used in the cyclic
calculations) (Vanstone, 3:13-28).

As to claim 8, Beaver as modified teaches:

a.   Characterized in that the calculation of each cycle comprises
calculation means for the first cycle and calculation means of cycles
subsequent to the first cycle (output of one processor becomes input to
the next processor and the cycles are repeated) (Beaver, p. 505, col. 2, 6th
paragraph).

b.   The calculation means generates the combination of the multiple
sequence alignment ElGamal cipher texts on the true value group ring and
the extended multiple sequence alignment ElGamal cipher texts on the
true value group ring with the calculation means of the zero-th cycle and
comprises reencryption public key generating means for generating a
public key used for reencryption by the calculation means of the first cycle,
data conversion means for converting the transmitted data, secret key
conversion means, and random number conversion means (ElGamal
shuffling includes transforming the order of the cipher texts) (Furukawa,
[0005, 0012]).

c.   The data conversion means is adapted to convert the combination
of the cipher texts that are the main data body with another combination of
multiple sequence alignment ElGamal cipher texts on the true value group
ring and extended multiple sequence alignment ElGamal cipher texts on
the true value group ring (elliptic curve ElGamal scheme is used in the
cyclic calculations) (Vanstone, 3:13-28).

d.   The secret key conversion means converts the secret key used for

the combination of the cipher texts that are the calculation result of the

data conversion means with a secret key corresponding to the public key

generated by the reencryption public key generating means (ElGamal

shuffling includes transforming the order of the cipher texts and

reencrypting the cipher texts for the next sequence of calculations)

(Furukawa, [0005, 0012]).

e.   The calculation result of the secret key conversion means

comprises a combination of multiple sequence alignment ElGamal cipher

texts on the true value group ring and extended multiple sequence

alignment ElGamal cipher texts on the true value group ring (elliptic curve

ElGamal scheme is used in the cyclic calculations) (Vanstone, 3:13-28).

f.   The random number conversion means is adapted to convert a

random number used for the combination of the cipher texts that are the

calculation results of the data conversion means (RNG or PRNG are used

in the calculation of random numbers used in calculating cryptographic

keys through hash functions) (Vanstone, 3:35-45).

g.   The calculation result of the random number conversion means

comprises a combination of multiple sequence alignment ElGamal cipher

texts on the true value group ring and extended multiple sequence

alignment ElGamal cipher texts on the true value group ring (the keys

generated by the RNG or PRNG are used for encryption purposes)

(Vanstone, 3:51-67).

As to claim 9, Beaver as modified teaches:

a.   Characterized in that the calculation means of the cycles

subsequent to the first cycle comprises of the calculation means of the

second cycles and the calculation means of cycles subsequent to the

second cycle (output of one processor becomes input to the next

processor and the cycles are repeated) (Beaver, p. 505, col. 2, 6th

paragraph).

b.   The data main body of the transmitted data and the data main body

calculated in the main calculation comprise a combination of multiple

sequence alignment ElGamal cipher texts on the true value group ring and

the extended multiple sequence alignment ElGamal cipher texts on the

true value group ring in the second calculation (ElGamal shuffling includes

transforming the order of the cipher texts) (Furukawa, [0005, 0012]).

c.   The calculation means of the second cycles cipher text conversion

means for converting the data main body of the transmitted data to

generate an ElGamal cipher text or an ellipse curve ElGamal cipher text

and partial decryption means for partially deciphering the cipher texts of

the data main body of the transmitted data (ElGamal shuffling includes

transforming the order of the cipher texts and reencrypting the cipher texts

for the next sequence of calculations) (Furukawa, [0005, 0012]).

18.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Applicant admitted prior art "The Round Complexity of Secure Protocols" by

Beaver et al. (hereinafter Beaver) in view of US Patent Application Publication

No. 2002/018172 to Furukawa and further in view of US Patent No. 6,195,433 to

Vanstone et al. (hereinafter Vanstone) as applied to claim 9 above, and further in

view of US Patent No. 6,792,533 to Jablon.

         As to claim 10, Beaver as modified teaches:

         a.   Characterized in that the calculation means of the cycles

         subsequent to the second cycle only comprises the calculation means of

         the third cycle (output of one processor becomes input to the next

         processor and the cycles are repeated) (Beaver, p. 505, col. 2, 6th

         paragraph).

Beaver as modified does not expressly mention a stopping condition. However,

in an analogous art, Jablon teaches:

         b.   The calculation means of the third cycle of the main calculation

         means outputs the transmitted data as it is and the validity proof

         generating means outputs a null string (the cycle of calculations stops

         when the stopping condition occurs when the calculation of g equals the

         generator) (Jablon, 13:47-67).

         Therefore, one of ordinary skill in the art at the time the invention was

made would have been motivated to implement the networked processor

computation protocol of Beaver as modified with the stopping condition of Jablon

in order to secure proof of knowledge of shared secrets as suggested by Jablon

(Jablon, 28-33).

Conclusion

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to WILLIAM S. POWERS whose telephone

number is (571)272-8573. The examiner can normally be reached on m-f 8:00-

5:00.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax

phone number for the organization where this application or proceeding is

assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

/William S. Powers/   William S. Powers
Examiner, Art Unit 2434   Examiner
                                              Art Unit 2434

11/8/2010